



Product Guide
Revision A

Endpoint Intelligence Agent 2.1.0

COPYRIGHT

Copyright © 2013 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS

McAfee, the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

	Preface	5
	About this guide	5
	Audience	5
	Conventions	5
	Find product documentation	6
1	Introduction	7
	How Endpoint Intelligence Agent works	7
	Endpoint Baseline Generator tool	11
	Determining your discovery method	12
2	Setting up Endpoint Intelligence Agent with ePolicy Orchestrator	13
	System requirements	13
	Download Endpoint Intelligence Management extension and Endpoint Intelligence Agent package	14
	Upload the Endpoint Intelligence Agent package	15
	Install the Endpoint Intelligence Management extension	15
	Deploy the Endpoint Intelligence Agent	15
	Upgrade the Endpoint Intelligence Agent	16
3	Configure Endpoint Intelligence Agent on Firewall Enterprise	17
	Configure certificates	17
	Generate the firewall certificate	18
	Sign the firewall certificate and export the CA certificate	18
	Load the certificates	19
	Configure certificates using SCEP	20
	Configure policy	21
	Create a policy	21
	Configure discovery options	22
	Modify the data channel Time to Live	23
	Configure advanced settings	23
	Assign policy to managed systems	25
	Firewall Enterprise setup	25
4	Configure Endpoint Intelligence Agent on NTBA	27
	Configure policy	27
	NTBA setup	27
5	Maintenance and troubleshooting	29
	View ePolicy Orchestrator reports	29
	View the Integrated Hosts report	29
	View the Gateway Status report	30
	View active hosts connected to Firewall Enterprise	30
	View related firewall audit	30
	View the Endpoint Intelligence Agent status	30
	Viewing the Endpoint Intelligence Agent logs	30

Log Collector tool	31
Troubleshooting tips	31
6 Frequently asked questions	35
Index	37

Preface

This guide provides the information you need to configure, use, and maintain your McAfee product.

Contents

- [About this guide](#)
- [Find product documentation](#)

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

*Book title, term,
emphasis*

Title of a book, chapter, or topic; a new term; emphasis.

Bold

Text that is strongly emphasized.

User input, code,
message

Commands and other text that the user types; a code sample; a displayed message.

Interface text

Words from the product interface like options, menus, buttons, and dialog boxes.

Hypertext blue

A link to a topic or to an external website.



Note: Additional information, like an alternate method of accessing an option.



Tip: Suggestions and recommendations.



Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.



Warning: Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

- 1 Go to the McAfee Technical Support ServicePortal at <http://mysupport.mcafee.com>.
- 2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	<ol style="list-style-type: none">1 Click Product Documentation.2 Select a product, then select a version.3 Select a product document.
KnowledgeBase	<ul style="list-style-type: none">• Click Search the KnowledgeBase for answers to your product questions.• Click Browse the KnowledgeBase for articles listed by product and version.

1

Introduction

McAfee® Endpoint Intelligence Agent is an endpoint solution that provides per-connection information to the supported network devices, namely, the McAfee® Firewall Enterprise (Firewall Enterprise) and the McAfee® Network Threat Behavior Analysis Appliance.

Contents

- ▶ *How Endpoint Intelligence Agent works*
- ▶ *Endpoint Baseline Generator tool*
- ▶ *Determining your discovery method*

How Endpoint Intelligence Agent works

Endpoint Intelligence Agent sends connection information, called *metadata*, that Firewall Enterprise uses for auditing and the NTBA appliance uses for enhanced malware detection capability.

Metadata

When Endpoint Intelligence Agent is installed on a host system, it monitors the system for any outgoing connections. When a connection attempt is made, McAfee EIA sends metadata information to Firewall Enterprise or to the NTBA appliance over an encrypted channel. This gives enough time for network device to process metadata and make it available at policy decision points before connection request packet is received.

Many network environments contain computers or servers that have multiple users logged on at the same time. The user information in the metadata allows the supported network devices to determine what users are associated with what connections, even if those connections are coming from the same IP address.

You can view the information collected by Endpoint Intelligence Agent providing better visibility on what users and applications are initiating connections on your network, while using the Firewall Enterprise or the NTBA appliance.

The executable file reputation in the metadata allows you to calculate the overall confidence level for an executable file connection. This enables the network device to configure response actions when malicious and unknown executables are detected on the network.

The metadata consists of the following information:

- Source and destination address
- Protocol
- Source and destination port

- The executable file name on the disk (full path) and hash of the process that generated the connection

This is an optional field and is sent only when file reputation is available.

- The user information associated with the process
- SID, user type (system users, local users, and domain users) and domain
- Executable file reputation
 - MD5 hash value
 - Confidence level
 - Heuristic bitmap
 - Evidence string
 - File name (same as the executable file name)
 - File description
 - File version
 - Signer name
 - Signed time
 - Global Threat Intelligence score
 - Product name

Executable file reputation

The McAfee EIA calculates the executable file reputation and stores it into a cache. MD5 is the key for storing the reputation of a file. The reputation is sent each time the information is available in the cache.

McAfee EIA receives notification when an application/process initiates traffic. It uses MD5 of the process to look up and check if the reputation is already available in the cache. If available, it sends the reputation information along with network and user information in the metadata. If the reputation is not available, it creates a background task. The task is picked up by one of four (recommended configuration) worker threads. Upon task completion, the corresponding thread updates the reputation cache.

McAfee EIA sends only mandatory fields of metadata every time a network connection is opened by an application. Optional parameters like heuristics are sent when they are available in the reputation cache.

The information of some of the loaded modules (DLLs) is sent, if its confidence level is above the configured reputation threshold.

You can configure the speed at which MD5 calculation happens inside McAfee EIA, the number of worker threads used, the confidence level to identify malicious files (reputation threshold). For more information see the section, *Configure advanced settings*.

Communication with a network device

As mentioned earlier, the Endpoint Intelligence Agent can communicate with two supported network devices, Firewall Enterprise and NTBA. At any given time, McAfee EIA can send metadata to only one network device for a particular source/destination network, based on configuration.

For information on configuring the network devices, see the following sections: *Configure Endpoint Intelligence Agent on NTBA* and *Configure Endpoint Intelligence Agent on Firewall Enterprise*.

The connection between Endpoint Intelligence Agent and the network device is a DTLS connection. The Endpoint Intelligence Agent uses heartbeat messages to detect the status of the connection. To save bandwidth, heartbeat is sent as part of metadata but not as a separate message. If Endpoint Intelligence Agent does not receive a response, even after sending three heartbeat messages, it declares the peer as dead.

When network traffic is generated, the reputation of the executable file is critical for the network device to configure response actions to prevent malicious files on the network. McAfee EIA monitors the executable files which send traffic from endpoints to the network device, and analyzes them and their associated libraries to calculate the file reputation.

The network devices receive the executable file reputation as part of the metadata, enabling them to determine the confidence level of the executable and configure response actions (such as raising alerts or blocking the files) when malicious and unknown executables are detected on the network. Thus facilitating clean traffic on the network and preventing malware intrusions.

The network devices also receive executable reputation by importing the baseline computer profile generated by the Endpoint Baseline Generator. For more details, see section *Endpoint Baseline Generator*.

The Endpoint Intelligence Agent leverages the McAfee® Global Threat Intelligence™ McAfee Global Threat Intelligence capability to provide file reputation information. The Endpoint Intelligence Agent does not talk to the GTI server directly. It uses the firewall/NTBA as a GTI proxy. It forwards the GTI queries to the network device. The network device talks to the GTI server and caches the response. It also forwards the response to the Endpoint Intelligence Agent, if it has requested for it.



Endpoint Intelligence Agent currently provides metadata for TCP and UDP connections over IPv4.

Endpoint Intelligence Agent is managed by McAfee® ePolicy Orchestrator® (ePolicy Orchestrator) and can be deployed to multiple systems.

The Endpoint Intelligence Manager configures certificates and policies for authentication of host. The Endpoint Intelligence Manager provides Host certificates to client computers to establish DTLS connection and can also manage the Network Integrity Agent version 1.0.0. For more information see section, Configure certificates.

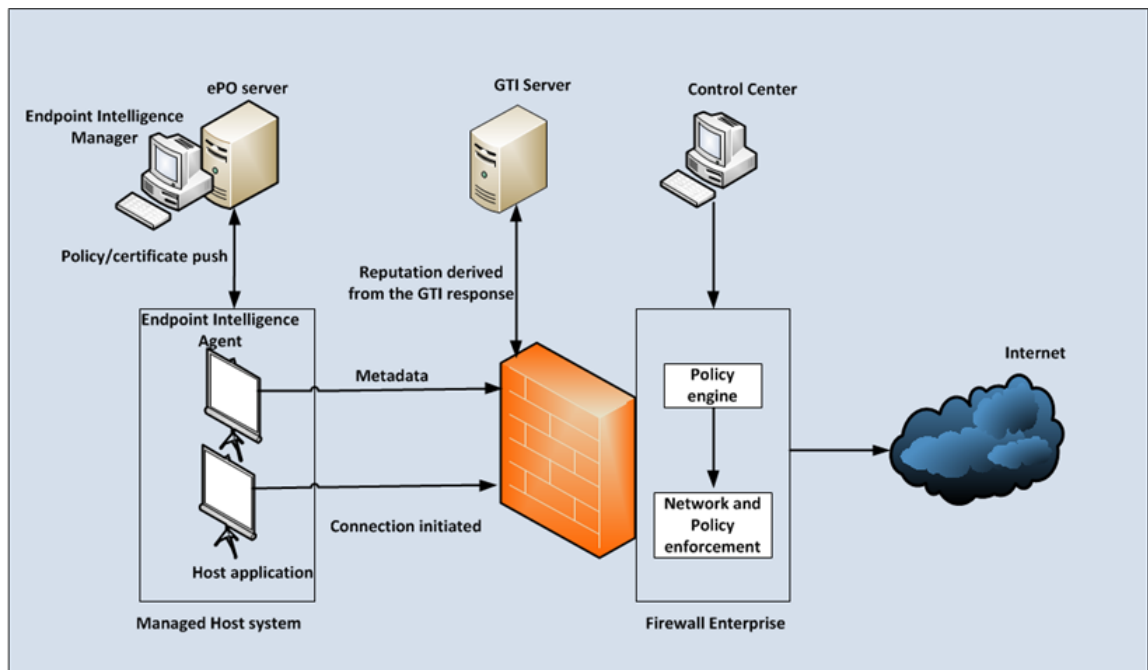


Figure 1-1 Integrating Endpoint Intelligence Agent with Firewall Enterprise

- ePolicy Orchestrator installs and configures the Endpoint Intelligence Agent settings on managed hosts.
- Firewall Enterprise is configured for Endpoint Intelligence Agent using the Admin Console. If your firewall is managed by Control Center, the firewall is configured on the Control Center Management Server.
- Endpoint Intelligence Agent sends metadata to Firewall Enterprise. User information and other metadata is used for auditing.
- Firewall updates its policies based on the metadata. The host system initiates the network connection for the application.

For more information to configure and view the reputation data, see the *McAfee Firewall Enterprise Product Guide*.

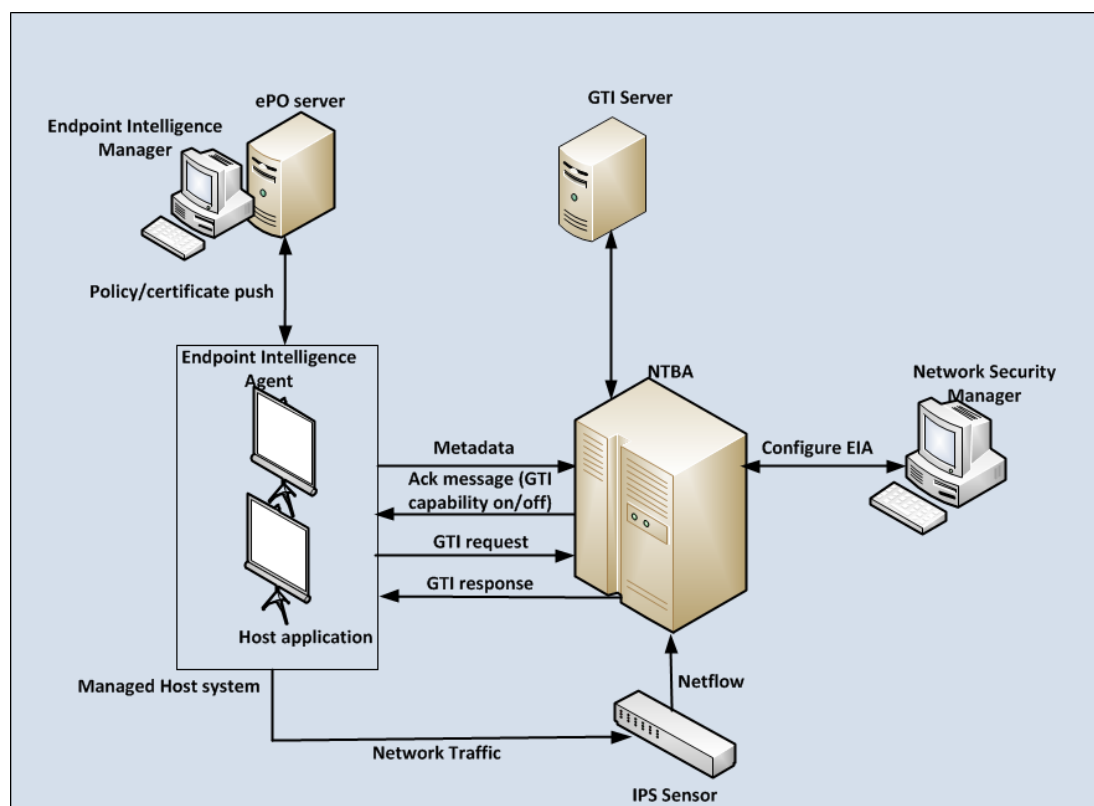


Figure 1-2 Integrating Endpoint Intelligence Agent with NTBA

- ePolicy Orchestrator installs and configures the Endpoint Intelligence Agent settings on managed hosts.
- The Network Security Manager (Manager) is used to configure McAfee EIA to establish connections between the NTBA appliance and the managed host systems.
- The NTBA appliance uses the configuration provided by the Manager and the ePO server to connect and authenticate with McAfee EIA endpoints.
- Endpoint Intelligence Agent sends metadata to the NTBA appliance. The NTBA uses the metadata for effective malware detection on the network.

For more information on configuring and managing McAfee EIA with NTBA, see the *McAfee NTBA Administration Guide*.

When the GTI capability is enabled on the NTBA appliance, McAfee EIA sends a GTI request consisting of the MD5. The NTBA communicates with the GTI server and sends a response to McAfee EIA consisting of the MD5 and the corresponding GTI value. Based on this response (GTI value) the confidence score in the reputation cache is refreshed.



Endpoint Intelligence Agent works with enterprise point-product installations on the host computers. Consumer point-product installations are not supported.

Endpoint Baseline Generator tool

The Endpoint Baseline Generator tool is used to implement a standard for endpoint hosts. The tool scans a computer, calculates the reputation for all the executable files on the system, and generates the baseline computer profile (an XML file) with the reputation details of each executable. This profile is uploaded from a computer to the NTBA and Firewall Enterprise, which use the same to evaluate the confidence level of the executables on the network, thereby securing network connections made by similar hosts, enabling Endpoint Intelligence Agent to report any deviations from that standard. The XML file generated by the tool associates the MD5 hash value, confidence level, and heuristic bitmap with each executable. This information provides the reputation to the network device to define a classification list consisting of the whitelisted, blacklisted, or unclassified (new or unknown executables) entries and monitors endpoint executable files.

You can import the baseline computer profile as generated by the tool or modify (add/delete) executable entries to this list. You can also modify executable entries as whitelisted or blacklisted.

Using the classification list, you can configure responses for these scenarios:

- A new executable file is detected
Unknown executable files are captured in the audit. You can set up an attack response to send an alert or strikeback.
- A blacklisted executable file is detected
You can identify vulnerable application versions as blacklisted on the classification list. You can set up an attack response to send an alert or strikeback.

You can edit the list of MD5 hashes generated, through import and export operations supported on the Firewall and on NTBA. For more information, see the *McAfee NTBA Administration Guide* and the *Firewall Enterprise Product Guide*.

Task

For option definitions, click **Help** in the interface.

- 1 Go to the **Endpoint Baseline Generator** tool. To scan specific directories, click **Include/Exclude Directories** and select the directories to be scanned.
- 2 Click **Scan**.
- 3 When the scan is complete, click **View Report**.

The XML report is displayed. The following is a sample of the MD5 associated with an application.

```
</MD5>
<MD5 value ='dadd090c2972d26f071f0ea0498fd6be' name="UWAKEON.EXE" version='7.0.711'>
  <ProductName>Workflow</ProductName>
  <ConfidenceLevel>2</ConfidenceLevel>
  <StaticBitmap>04aaaaaaaa0200000000000000000000</StaticBitmap>
</MD5>
```

The confidence levels associated with an executable are specified in numeric values. Each of these values corresponds to the following confidence levels.

- 0 - Unknown
- 2 - Very Low Risk
- 3 - Low Risk
- 4 - Medium Risk
- 5 - High Risk
- 6 - Very High Risk



- The confidence levels can't be modified and are imported as part of the baseline computer profile.
- You can cancel the scan in the middle and still generate a valid XML file to be imported by the target device.

4 To export and save the results in an XML format, click **Export**.

5 To view the details of the scan, click **View Results**.



The Endpoint Baseline Generator supports scanning external hard drives with fixed media, for example, a hard disk drive or a flash drive.

Determining your discovery method

Host systems running Endpoint Intelligence Agents have two ways of determining the gateway to send connection metadata to: *static* and *dynamic*.

Systems running Endpoint Intelligence Agent can have a combination of static and dynamic configurations. When a connection attempt is made, Endpoint Intelligence Agent will check its route configuration using the static or the dynamic mode.



Firewall Enterprise uses both static and dynamic modes. NTBA uses only the static mode.

- **Static** — If the connection has a destination IP address (Firewall Enterprise) / source IP address (NTBA) that matches a route entry, McAfee EIA sends metadata to the specified gateway IP address for that route.
- **Dynamic** — If the connection has a destination IP address that does not match any McAfee EIA route entries, it only sends metadata when it receives a request.

2

Setting up Endpoint Intelligence Agent with ePolicy Orchestrator

Install the Endpoint Intelligence Management Extension, check in the Endpoint Intelligence Agent package, and deploy Endpoint Intelligence Agent to managed systems.

Contents

- *System requirements*
- *Download Endpoint Intelligence Management extension and Endpoint Intelligence Agent package*
- *Upload the Endpoint Intelligence Agent package*
- *Install the Endpoint Intelligence Management extension*
- *Deploy the Endpoint Intelligence Agent*
- *Upgrade the Endpoint Intelligence Agent*


System requirements

Make sure your Firewall Enterprise, McAfee Network Threat Behavior Analysis (NTBA), ePolicy Orchestrator, and managed systems meet the requirements.

The following are the product requirements for Endpoint Intelligence Agent 2.1.0.

Product	Supported version
ePolicy Orchestrator server	Version 4.6.5 or later
McAfee Agent	Version 4.8.0 Patch 1 or later
Endpoint Intelligence Management Extension	Version 2.1.0

The following are the integrated product requirements for Endpoint Intelligence Agent 2.1.0.

Product	Supported version
Firewall Enterprise Control Center Firewall Enterprise	Version 5.3.1 or later. Version 8.3.1 with the latest P-patch, version 8.3.2 or later. <div>  <ul style="list-style-type: none"> Version 8.3.1 with the latest P-patch McAfee EIA works only with the Network Integrity Agent 1.0.0 features. Version 8.3.1 without the latest P-patch McAfee EIA does not communicate with the Firewall Enterprise. </div>
Network Threat Behavior Analysis (NTBA)	Version 8.0.5.6 or later.



Firewall Enterprise ePO extension 5.3.0 or earlier version cannot co-exist with Endpoint Intelligence Manager ePO extension.

- Endpoint Intelligence Agent runs on the following Microsoft operating systems:



Both 32-bit and 64-bit operating systems are supported.

- Windows XP Service Pack 2 and later
- Windows Server 2003 R2 Service Pack 2 and later
- Windows 7
- Windows Server 2008 R2 (only 64 bit)
- Windows Server 2003 Service Pack 2 and later
- Windows Server 2008



McAfee recommends running Endpoint Intelligence Agent on systems with at least 2 GB of RAM.

Download Endpoint Intelligence Management extension and Endpoint Intelligence Agent package

Download the Endpoint Intelligence Management Extension and the Endpoint Intelligence Agent package to the ePolicy Orchestrator server.

Before you begin

Locate your grant number.

Task

- In a web browser, go to www.mcafee.com/us/downloads.
- Enter your grant number, then go to the appropriate product and version.
- Download the eia_epo_deploy_210.zip file.
- Download the eim_epo_extension_210.zip file.
- [Optional] Download the eim_epo_extension_help_210.zip file.

Upload the Endpoint Intelligence Agent package

Upload the Endpoint Intelligence Agent package to the ePolicy Orchestrator server. This package contains the files necessary to install Endpoint Intelligence Agent on managed systems.

Task

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, select **Menu | Software | Master Repository**.
- 2 Click **Check In Package**. The **Check In Package** wizard appears.
- 3 In the **Package type** list, select **Product or Update (.ZIP)**, then browse and select the Endpoint Intelligence Agent package file.
- 4 Click **Next**.
- 5 Click **Save**.

The package is added to the Master Repository.

Install the Endpoint Intelligence Management extension

Install the Endpoint Intelligence Management extension from your download location to your ePolicy Orchestrator server.

Task

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, select **Menu | Software | Extensions**.
- 2 At the bottom of the **Extensions** pane on the left side of the **Extensions** page, click **Install Extension**. The **Install Extension** window appears.
- 3 Browse to the Endpoint Intelligence Agent Management extension file you downloaded from the McAfee downloads page.
- 4 Click **Open** to select the file, then click **OK** to proceed with the selection.
- 5 Click **OK** to install the extension.



To complete the installation process, you do *not* need to reboot the machine. Reboot is required after uninstallation.

Deploy the Endpoint Intelligence Agent

Deploy Endpoint Intelligence Agent to managed systems.

Task

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, select **Menu | Policy | Client Task Catalog**. The **Client Task Catalog** area appears.
- 2 Click **New Task**. The **New Task** window appears.

- 3 In the **Task Types** list, select **Product Deployment**.
- 4 Click **OK**. The **Client Task Catalog: New Task - McAfee Agent: Product Deployment** window appears.
- 5 In the **Task Name** field, enter a name for the task.
- 6 From the **Products and components** menu, select **Endpoint Intelligence Agent 2.1.0**.
- 7 Click **Save**.
- 8 Run the task.
 - a Click the **System Tree** icon. The **Systems** tab appears.
 - b Select the systems to deploy Endpoint Intelligence Agent to.
 - c Select **Actions | Agent | Run Client Task now**. The **Run Client Task Now** page appears.
 - d In the **Task Type** column, select **Product Deployment**, and in the **Task Name** column, select the task you created.
 - e Click **Run Task Now**.

Upgrade the Endpoint Intelligence Agent

You can upgrade from Endpoint Intelligence Agent 2.0.0 to Endpoint Intelligence Agent 2.1.0



Upgrade from an older version of the Endpoint Intelligence Agent (previously known as Network Integrity Agent) is not supported.

Task

- 1 Download the latest Endpoint Intelligence Agent package .zip file.
- 2 Upload the package into the ePolicy Orchestrator repository.
- 3 Deploy the agent to the target machine.

Endpoint Intelligence Agent and Firecore files upgrade to the latest version. All upgrade attempts generate logs in the installation directory.



- If the upgrade fails, Endpoint Intelligence Agent restores to the previous version.
- To complete the upgrade process, you do *not* need to reboot the machine.

3

Configure Endpoint Intelligence Agent on Firewall Enterprise

To configure Endpoint Intelligence Agent on Firewall Enterprise, follow the procedures in this section.

Contents

- [Configure certificates](#)
- [Configure policy](#)
- [Firewall Enterprise setup](#)

Configure certificates

Certificate configuration is necessary for the encrypted communication between Firewall Enterprise and McAfee EIA.



The certificate configuration is *not* required for NTBA.



If you are using Control Center to manage your firewall, see the *McAfee Firewall Enterprise Control Center Product Guide, Certificates* chapter.

The certificate process consists of these high-level steps:

- 1 In the firewall, generate and export the certificate for McAfee EIA.
- 2 Sign that certificate in the Endpoint Intelligence Management extension.
- 3 Export the ePolicy Orchestrator certificate authority (CA) certificate.
- 4 Load the signed certificate and the CA certificate into the firewall.

When creating certificates, they must meet these requirements:

- Public key lengths must be 4096 bits or lower.
- The host certificate used by McAfee EIA must be signed by the same certificate authority that generated the CA certificate.

Tasks

- [Generate the firewall certificate on page 18](#)
Create and export a firewall certificate to be signed by ePolicy Orchestrator.
- [Sign the firewall certificate and export the CA certificate on page 18](#)
Use ePolicy Orchestrator to sign the firewall certificate and export the ePolicy Orchestrator CA certificate.
- [Load the certificates on page 19](#)
Load the signed certificate and the ePolicy Orchestrator CA certificate to Firewall Enterprise.
- [Configure certificates using SCEP on page 20](#)
If you do not want to use the ePolicy Orchestrator CA to sign the certificate, you can use the Simple Certificate Enrollment Protocol (SCEP) instead.

Generate the firewall certificate

Create and export a firewall certificate to be signed by ePolicy Orchestrator.

Task

For option definitions, click **Help** in the interface.

- 1 From the Firewall Enterprise Admin Console, select **Maintenance | Certificate/Key Management | Firewall Certificates**.
- 2 Click **New**. The **Firewall Certificates: Create New Certificate** window appears.
- 3 In the **Certificate name** field, enter a name for the certificate.
- 4 In the **Distinguished name (DN)** field, enter a distinguished name.
- 5 From the **Submit to CA** menu, select **Manual PKCS 10**.
- 6 Click **Browse** to specify the name and location to export the certificate to.
- 7 From the **Format** menu, select **PKCS10**.
- 8 Click **Add**. A success message appears.
- 9 Click **OK**.

The certificate is exported to the specified location.


Sign the firewall certificate and export the CA certificate

Use ePolicy Orchestrator to sign the firewall certificate and export the ePolicy Orchestrator CA certificate.

Task

For option definitions, click **?** in the interface.

- 1 From the ePolicy Orchestrator console, select **Menu | Configuration | Server Settings**. The **Server Settings** area appears.
- 2 Select **Endpoint Intelligence Settings**, then click **Edit**. The **Edit Endpoint Intelligence Settings** page appears.
- 3 Modify the following server settings for McAfee.

Option	Definition
Retention Interval	Specifies the number of days ePolicy Orchestrator keeps the Gateway Status reports sent from the McAfee EIA.
'Time to Live' for Data channel packets	Specifies the amount of time to live for data channel packets. The time range is 1 to 1440 minutes. By default, this is set to 10 minutes.
Certificate	<p>Specifies whether ePolicy Orchestrator uses self-signed certificate as CA certificate to sign certificates for the endpoint or an external SCEP server. Select one of these options.</p> <ul style="list-style-type: none"> • ePO generated self signed certificate — Specifies the ePO extension certificate used to sign the certificate for the endpoint. <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;">  ePO extension certificate is generated when it is installed. Re-installation will regenerate the certificate. </div> <ul style="list-style-type: none"> • CA certificate — Specifies the SCEP CA that ePO extension uses to generate certificates for endpoints.
Certificate Options	<p>When you select the ePO generated self signed certificate option, upload the CSR file exported from firewall and get the certificate signed.</p> <ul style="list-style-type: none"> • Validity period (in years) for generated host certificates: — Specifies the validity for the host certificates generated. • Browse — Specifies the firewall certificate to be signed. • Sign Certificate — Specifies signing the uploaded firewall certificate. • Download Endpoint Intelligence CA certificate: — Downloads the ePO extension CA certificate. This certificate must be added as CA in Firewall. <p>When you select the CA certificate option, enter SCEP server credentials and save the settings.</p> <ul style="list-style-type: none"> • CA SCEP Url — Specifies the SCEP server url address. • CA ID — Specifies the SCEP server ID. • SCEP Password — Specifies the password to access the SCEP server. • Test Connection — Tests the validity of the SCEP server address and user credentials. • Download test pkcs12 — Downloads a test PKCS12 file for testing purposes. • Get CA Cert — Downloads the SCEP server's CA certificate.



McAfee EIA does not support certificates signed with SHA-256 with RSA encryption algorithm.

Load the certificates

Load the signed certificate and the ePolicy Orchestrator CA certificate to Firewall Enterprise.

Task

For option definitions, click **Help** in the interface.

- 1 From the Firewall Enterprise Admin Console, select **Maintenance | Certificate/Key Management**.
- 2 Load the signed certificate.
 - a Click the **Firewall Certificates** tab.
 - b In the **Certificates** list, select the certificate, then click **Load**. The **Firewall Certificates: Load Certificate for PKSC10 Request** window appears.
 - c For **Certificate Source**, select **File**.
 - d Click **Browse** and select the signed certificate file.
 - e Click **OK**.
 - f On the **Firewall Certificates** tab, select the certificate and verify that the status is **SIGNED**.
- 3 Load the ePolicy Orchestrator CA certificate.
 - a Click the **Certificate Authorities** tab.
 - b Click **New | Single CA**. The **Certificate Authorities: New Certificate Authority** window appears.
 - c In the **Name** field, enter a name for the certificate.
 - d Click **Browse** and select the CA certificate file.
 - e Click **Add**.

Configure certificates using SCEP

If you do not want to use the ePolicy Orchestrator CA to sign the certificate, you can use the Simple Certificate Enrollment Protocol (SCEP) instead.

Task

- 1 From the ePolicy Orchestrator console, select **Menu | Configuration | Server Settings**. The **Server Settings** area appears.
- 2 Select **Endpoint Intelligence Settings**, then click **Edit**. The **Edit Endpoint Intelligence Settings** page appears.
- 3 Configure SCEP settings.
 - a Select **CA Certificate**.
 - b Enter the information in the **CA SCEP Url**, **CA Id** and **Scep Password** fields.
 - c Click **Test Connection** to verify the information. A success message appears.
 - d Click **Get CA Cert**.
- 4 On the Firewall Enterprise Admin Console, select **Maintenance | Key Management**.
- 5 Configure the CA certificate.
 - a Click the **Certificate Authorities** tab.
 - b Click **New**. The **Certificate Authorities: New Certificate Authority** window appears.
 - c From the **Type** drop-down list, select **SCEP**.

- d Enter the information for the CA certificate.
 - e Click **Add**.
 - f Click **Get CA Cert** to get the Distinguished Name details.
- 6 Configure the firewall certificate.
 - a Click the **Firewall Authorities** tab.
 - b Click **New**. The **Firewall Certificates: Create New Certificate** window appears.
 - c From the **Submit to CA** drop-down list, select the name of the CA certificate you configured on the firewall.
 - d Click **Add**.
 - e Enter the information for the certificate.
- 7 Save your changes.

Configure policy

Configure the shared key and route discovery information. You can edit or duplicate an existing policy, or create a new policy.

Two preconfigured policies are generated for Endpoint Intelligence Agent:

- **McAfee Default** is read-only and cannot be deleted. It can be duplicated.
- **My Default** is fully editable.

Tasks

- [Create a policy on page 21](#)
If you do not want to use the preconfigured policy, create a policy.
- [Configure discovery options on page 22](#)
Edit a policy to specify optional route and discovery information for managed systems.
- [Modify the data channel Time to Live on page 23](#)
The data channel Time to Live controls when the connection between ePolicy Orchestrator and Endpoint Intelligence Agent times out. On networks with slower connectivity, you might need to increase the Time to Live.
- [Configure advanced settings on page 23](#)
Edit a policy to make advanced configurations, such as logging and connection settings.
- [Assign policy to managed systems on page 25](#)
For Endpoint Intelligence Agent to communicate with Firewall Enterprise/NTBA, policy must be applied to managed systems.

Create a policy

If you do not want to use the preconfigured policy, create a policy.

Task

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, select **Menu | Policy | Policy Catalog**. The **Policy Catalog** area appears.
- 2 In the **Product** list, select **Endpoint Intelligence Agent 2.1.0**.

- 3 Click **New Policy**. The **New Policy** window appears.
- 4 Choose a policy in the **Create a policy based on this existing policy** list.
- 5 Enter a name in the **Policy Name** field.
- 6 [Optional] Enter a description in the **Notes** field.
- 7 Click **OK**.

The new policy appears in the **Name** column in the **Policy Catalog** area.

Configure discovery options

Edit a policy to specify optional route and discovery information for managed systems.

Specifying route discovery information provides Endpoint Intelligence Agent with the Firewall Enterprise/NTBA IP address needed for sending metadata to a particular network route.

If you do not configure firewall information for a particular route, McAfee EIA automatically discovers the firewall for that route provided the firewall is deployed in dynamic mode.

Task

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, select **Menu | Policy | Policy Catalog**. The **Policy Catalog** area appears.
- 2 In the **Product** list, select **Endpoint Intelligence Agent 2.1.0**.
- 3 In the **Name** column, click the policy to configure. The **General Settings** tab appears.
- 4 In the **Shared Key** field, enter the key to decrypt the redirected messages. This key must be same between the firewall/NTBA and endpoint. The shared key must contain a minimum of 16 characters.
- 5 In the **Device Type** list, select **McAfeeFirewall Enterprise** or **NTBA**.
- 6 Specify the following information on the routes on which Endpoint Intelligence Agent sends information to the firewall/NTBA.

Option Definition	
Routes	<ul style="list-style-type: none"> • Destination — Specifies the server IP to which communication request is sent. Endpoint Intelligence Agent sends connection information of IPs in the specified subnet to Firewall Enterprise. • Source — Specifies the host IP. Endpoint Intelligence Agent sends connection information of IPs in the specified subnet to NTBA. • Subnet Mask — Specifies the subnet mask value for the network. • Device IP — Specifies the IP address of the Firewall Enterprise/NTBA appliance that needs endpoint information from the Endpoint Intelligence Agent. • Port — The default port used by Firewall Enterprise/NTBA is 9008.

- 7 Click **Add Route**.



To remove a route, select the entry and click **Remove Route**.

- 8 Configure exemptions for specific destinations as needed.

Example: You have a subnet configured for route discovery, but you don't want to send metadata for a particular host in that network.

- a Enter the network address and subnet mask as you did in steps 4 and 5, but leave the **Device IP** and **Port** fields empty.
 - b Select **Exempt Route**.
 - c Click **Add Route**.
- 9 When you are done entering discovery options, click **Save**.
- Click **Duplicate** to create a copy of the **My Default** or **McAfee Default** settings. Click **Cancel** to return to the **Policy Catalog** page.

See also

[Determining your discovery method on page 12](#)

Modify the data channel Time to Live

The data channel Time to Live controls when the connection between ePolicy Orchestrator and Endpoint Intelligence Agent times out. On networks with slower connectivity, you might need to increase the Time to Live.

Task

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, select **Menu | Configuration | Server Settings**. The **Server Settings** area appears.
- 2 Select **Endpoint Intelligence Settings**, then click **Edit**. The **Edit Endpoint Intelligence Settings** page appears.
- 3 In the 'Time to Live' for Data channel packets field, enter the amount of time in minutes. Valid values are 1–1440. The default is 10 minutes.

Configure advanced settings

Edit a policy to make advanced configurations, such as logging and connection settings.

Task

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, select **Menu | Policy | Policy Catalog**. The **Policy Catalog** area appears.
- 2 In the **Product** list, select **Endpoint Intelligence Agent 2.1.0**.
- 3 In the **Name** column, click the policy to configure. The **General Settings** tab appears.
- 4 In the **Device Type** list, select **McAfeeFirewall Enterprise** or **NTBA**.
- 5 Click the **Advanced Settings** tab. This tab specifies the default runtime parameters and settings for Endpoint Intelligence Agent. We recommend that you keep these at default values.
- 6 Configure the following settings as needed.

Option	Definition
Log Level	Specifies the logging level for the Endpoint Intelligence Agent. By default, this is selected as Error. You can select other logging levels like Fatal, Error, Warn, and Debug based on your need.
Log Numbers	Specifies the number of times the log files are rotated in the system. After this limit, the log files are removed. For example, if the log number is 0, the old versions are removed. The default value is 10.
Log Size	Specifies the limit of log file size in MB. Once the log files reach this log size, they are rotated as per the Log Numbers . The maximum log file size is 2048 MB. By default, this value is set to 10 MB.
Firewall Retry Interval	[Error occurrence] Specifies the waiting time in milliseconds before retrying a connection to the gateway. The maximum time limit is 5000 milliseconds. By default, this value is set to 1000.
Firewall Recovery Interval	[Recovery from a slow firewall connection] Specifies the time in milliseconds prior to reducing the delay on sending packets to the firewall. The maximum time limit is 60000 milliseconds. By default, this value is set to 3000 milliseconds.
Firewall Backoff Percentage	[Slow firewall connection detected] Specifies the percentage increase in the current delay period. This increases the amount of time Endpoint Intelligence Agent gets to send connection information to firewall and for firewall to process this connection information. The percentage range is 200 to 999. By default, this value is set to 500.
Firewall Backoff Maximum Interval	Specifies the amount of time to send and process the connection information. The time range is 5 to 100 milliseconds. By default, this value is set to 10 milliseconds.
Enable Discovery	Specifies the firewall automatically discovers endpoints that have Endpoint Intelligence Agent. By default, this checkbox is deselected.
DTLS Keep Alive	Specifies the intervals in seconds at which an endpoint sends acknowledgments to the firewall. <ul style="list-style-type: none"> • If the Enable Discovery of Agent by Firewall checkbox is deselected, the time range is 10 to 60 seconds. By default, this value is set to 20 seconds. • If the Enable Discovery of Agent by Firewall checkbox is selected, the time range is 60 to 300 seconds. By default, this is set to 180 seconds.
Firewall Session Expiry	Specifies the maximum amount of time in minutes for which the firewall session exists. After this time, the session times out. The session time range is 10 to 300 minutes. By default, this value is set to 60 minutes.
Ignore Virtual Traffic	Specifies ignoring traffic from virtual adaptors. By default, this checkbox is selected.
Reputation Threshold	Specifies the reputation score below which an executable is considered malicious. By default, this value is set to Medium.
GTI Expiry	Specifies the time after which the GTI cache entries expire. By default, this value is set to 3600 seconds.
MD5 Relaxation	Used to configure the speed at which MD5 calculation happens inside McAfee EIA. Increasing the MD5 relaxation reduces the CPU used by McAfee EIA processes, also slowing down the reputation computation. The MD5 Relaxation is calculated in milliseconds. The default value is 20.

Option	Definition
Thread Count	Used to configure the number of worker threads used by McAfee EIA to compute reputation. Reducing the thread count reduces the performance of McAfee EIA (used for debugging purposes). The default value is 4.
Show Configuration GUI	Specifies if configuration information must be displayed on the endpoint interface. By default, this checkbox is deselected.



McAfee recommends not to change the **MD5 Relaxation** and **Thread Count** values unless required. These parameters, if not set appropriately, can reduce the performance of McAfee EIA.

- Click **Save** to save the modified settings.

Click **Duplicate** to create a copy of the **My Default** or **McAfee Default** settings. Click **Cancel** to return to the **Policy Catalog** page.

Assign policy to managed systems

For Endpoint Intelligence Agent to communicate with Firewall Enterprise/NTBA, policy must be applied to managed systems.

Task

For option definitions, click ? in the interface.

- From the ePolicy Orchestrator console, select **Menu | Systems | System Tree**. The **Systems** tab appears.
- Select the systems to apply policy to.
- Select **Actions | Agent | Set Policy & Inheritance**. The **Assign Policy** page appears.
- From the **Product** menu, select **Endpoint Intelligence Agent 2.1.0**.
- From the **Policy** menu, select the policy.
- Click **Save**.

Firewall Enterprise setup

You can enable McAfee EIA on the Firewall Enterprise using the Admin console.

For more information on configuring and managing McAfee EIA on the Firewall Enterprise, see section, *Policy < McAfee EIA* in the *McAfee McAfee Firewall Enterprise Control Center Product Guide*.

4

Configure Endpoint Intelligence Agent on NTBA

To configure Endpoint Intelligence Agent on NTBA appliance, follow the procedures in this section.

Contents

- [Configure policy](#)
- [NTBA setup](#)

Configure policy

Configure the shared key and route discovery information. You can edit or duplicate an existing policy, or create a new policy.

Two preconfigured policies are generated for Endpoint Intelligence Agent:

- **McAfee Default** is read-only and cannot be deleted. It can be duplicated.
- **My Default** is fully editable.

See also

[Configure policy on page 21](#)

NTBA setup

You can enable McAfee EIA integration on the NTBA appliance using the McAfee® Network Security Manager (Manager).

For more information on setting up, configuring and managing McAfee EIA on the NTBA appliance, see section, *Integrating with McAfee Endpoint Intelligence Agent* in the *McAfee NTBA Administration Guide*.

5

Maintenance and troubleshooting

You can use a variety of reports and logs to monitor the status of host agents and troubleshoot communication or operational problems.

Contents

- [View ePolicy Orchestrator reports](#)
- [View active hosts connected to Firewall Enterprise](#)
- [View related firewall audit](#)
- [View the Endpoint Intelligence Agent status](#)
- [Viewing the Endpoint Intelligence Agent logs](#)
- [Log Collector tool](#)
- [Troubleshooting tips](#)

View ePolicy Orchestrator reports

ePolicy Orchestrator provides two built-in reports to check the connection status of Endpoint Intelligence Agent on managed systems.

Tasks

- [View the Integrated Hosts report on page 29](#)
The Integrated Hosts report lists all managed systems with an active Endpoint Intelligence Agent.
- [View the Gateway Status report on page 30](#)
The Gateway Status report lists agent hosts that have problems communicating with the Firewall Enterprise gateway.

View the Integrated Hosts report

The Integrated Hosts report lists all managed systems with an active Endpoint Intelligence Agent.

Task

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, select **Menu | Reporting | Queries & Reports**. The **Queries & Reports** area appears.
- 2 Select the **Network Integrity: Integrated Hosts** report, then click **Run**. The **Network Integrity: Integrated Hosts** page appears.
- 3 When you are finished viewing the report, click **Close**.

View the Gateway Status report

The Gateway Status report lists agent hosts that have problems communicating with the Firewall Enterprise gateway.

Task

For option definitions, click ? in the interface.

- 1 From the ePolicy Orchestrator console, select **Menu | Network | Gateway Status report**. The **Enterprise Firewalls** area appears.
- 2 When you are finished viewing the report, click **Close**.

View active hosts connected to Firewall Enterprise

There are two methods of viewing active hosts connected to Firewall Enterprise. For more information, see the *Firewall Enterprise Product Guide*.



If you are using Control Center to manage your firewall, see the *McAfee Firewall Enterprise Control Center Product Guide, Generate Active Hosts Report*.

View related firewall audit

From the firewall dashboard, access firewall audit entries related to Endpoint Intelligence Agent. For more information, see the *McAfee Firewall Enterprise Product Guide*.

View the Endpoint Intelligence Agent status

The McAfee EIA running on host systems has a utility that displays information such as connection status and settings.

Task

- 1 From the Endpoint Intelligence Agent Configuration utility, click **View Status**. The **Endpoint Intelligence Agent Status** window displays.
- 2 When finished, click **OK** to close the window.

Viewing the Endpoint Intelligence Agent logs

Endpoint Intelligence Agent writes errors and debugging information to several local log files on the host machine. These log files might be requested when working with technical support.

- Agent information is logged to mfe-eia.log. This file is located in the install directory.
- User interface information is logged to mfe-eiaconfig.log. This file is located in the install directory.
- Installation information is logged to EIAInstallation.log. The location of this file varies depending on the system user, but it is commonly found in C:\Windows\Temp\McAfeeLogs.
- McAfee EIA-ePO communicator service information is logged to mfe-eiaepocom.log.
- Endpoint Baseline Generator information is logged to mfe-ebg.log.

Log Collector tool

You can collect logs using LogCollector.exe in the Endpoint Intelligence Agent install folder. This file is found in C:\Program Files\McAfee\Endpoint Intelligence Agent\x86. The logs are generated in the EiaDiagnosisLogs.CAB folder. The location of this folder varies depending on the system user; it is found in the x86 folder in the 32-bit operating system and in the x64 folder in the 64-bit operating system.

The following files are copied from the installation directory (different for 32-bit and 64-bit operating systems):

- firecore.log
- mfe-eia.log
- mfe-eia.log.[1-10]
- mfe-ebg.log
- mfe-eiaepocom.log
- mfe-eiaconfig.log
- Syscore.etl
- cachedReputation.txt
- install.log
- EIAUnInstall.log
- EIAInstallation.log
- EIAUninstall.log

The following files are also copied:

- %systemroot%\Temp\McAfeeLogs\EIAInstallation.log
- %systemroot%\Temp\McAfeeLogs\EIAUninstall.log
- Files under %programdata%\HYPERLINK "file:///\\McAfee\Common%20Framework\DB" \McAfee \Common Framework\DB\
- Files under %AppData%\HYPERLINK "file:///\\McAfee\Common%20Framework\DB" \McAfee \Common Framework\DB\

Troubleshooting tips

Some troubleshooting tips while using McAfee EIA are given in the following table.

Problem	Solution
The McAfee EIA Service does not start	<p>In case the McAfee EIA Service does not start:</p> <ul style="list-style-type: none"> • Check if Firecore service is running (start if it is not running) • In case VSE is present, disable Access Protection to start the Firecore service. • Check if the McAfee EIA service is running (start if it is not running). <p>Verify the status of Firecore installation. If there is a problem, try reinstalling Firecore from the installation directory:</p> <ul style="list-style-type: none"> • Uninstall Firecore: mfehidin.exe -u -x nia.xml -l firecore.log • Install Firecore: mfehidin.exe -i -x nia.xml -l firecore.log
Reputation not received on firewall for an application even after multiple connections.	<p>Dump the reputation cache:</p> <ul style="list-style-type: none"> • In memory reputation cache can be dumped by creating the following registry key: <ul style="list-style-type: none"> • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\Endpoint Intelligence Agent\Configured\DumpCache • It must be REG_MULTI_SZ. • Set its value to 1. • Reputation will be written to cachedReputation.txt in the installation directory, for example, C:\Program Files (x86)\McAfee\Endpoint Intelligence Agent\x64.
Troubleshooting ePO deployments	<p>To enable manual configuration for troubleshooting ePO deployments:</p> <ul style="list-style-type: none"> • Go to key: HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\Network Integrity Agent\Settings • Change ShowGuiButton to 1. • Reopen the McAfee EIA configuration dialog box.
If DTLS connection is not established between EIA and the network device	<p>Check if the certificate verification is successful and the shared key is correct in the status screen.</p>
Issues related to routing	<p>Verify the routing information. The current routing table is printed in the logs every time a new route is added.</p>
Issues related to MA	<p>View the MA status, go to McAfee\Common framework, and run cmdagent.exe /s.</p>
Issues with the installer	<p>Collect the following log files for information:</p> <ul style="list-style-type: none"> • ePO, eia install log • etlTrace, mfe-eiaepocom and mfe-eia logs • mfe-eiaconfig.log
Issues with the McAfee EIA service	<p>In case of issues with the McAfee EIA service:</p> <ul style="list-style-type: none"> • Enable debug logs for McAfee EIA service by changing the log level to debug in the ePO advanced policy. • Collect all mfe-eia.log and mfe-eiaepocom logs. • Dump the reputation cache by following the preceding point. • If possible, use Wireshark to analyze captures on the host.

Problem	Solution
Issues with the EIM extension	<p>In case of issues with the EIM extension:</p> <ul style="list-style-type: none"> • Provide the policy configuration. • Provide the browser version details. • In case of certificate issues, provide the ePO Audit logs. • Collect the ePO MER logs. For more information, see KB59385.
Issues with the McAfee EIA/communicator crash	<p>In case of issues with the McAfee EIA/communicator crash:</p> <ul style="list-style-type: none"> • Collect the crash dump from crashes folder in the installation directory. • Provide the relevant windows event viewer log. • Enable debug logs for McAfee EIA service by changing the log level to debug in the ePO advanced policy. • Collect all mfe-eia.log and mfe-eiaepocom logs. • Collect the ePO, eia install log files. • Collect the etlTrace, mfe-eiaepocom and mfe-eia logs. • If possible, provide the relevant crash .exe file, for example, mfe-ebg64.exe or mfe-eiaepocom.exe. • Provide the MA debug logs in case of ePolicy Orchestrator communicator crash.
While using the LogCollector tool, I receive the error, copying EIA diagnosis logs to C:\Program Files (x86)\McAfee\Endpoint IntelligenceAgent\x64\EiaDiagnosisLogs.CAB file not found - DB.	<p>The LogCollector tool copies files from the %programdata%\McAfee\Common Framework\DB\ and the %AppData%\McAfee\Common Framework\DB\ folders. Check these folders; in their absence this error occurs.</p>

6

Frequently asked questions

This section answers some of the frequently asked questions about Endpoint Intelligence Agent.

Question 1

When McAfee EIA switches the DTLS connection from one network device to another, the older connection continues to be displayed in the status screen as connected. Why?

Answer 1

When a route is added, McAfee EIA connects to a network device and starts sending metadata. The status screen displays that the connection is up.

Since the connection between McAfee EIA and the network device is UDP connection over TLS, that is, DTLS, McAfee EIA uses heart beat messages to detect the status of the connection. To save bandwidth, heartbeat is sent as part of metadata but not as a separate message. If McAfee EIA does not receive a response, even after sending three heartbeat messages, it declares the peer as dead.

When a route gets changed, McAfee EIA connects to a new network device and starts sending metadata. It does not have any data that needs to be sent to the older device. Since there is no data, there is no way of sending a heartbeat message. So the status of the older connection remains in the same state. The connection status screen shows two rows. One for the previous connection and the other for the current connection.

Question 2

While trying to uninstall McAfee EIA manually from the Control Panel, the uninstall fails with the error message, "unable to open install log file and to check for permissions". Why?

Answer 2

This is a known issue on Windows 7. The available workaround is to stop and restart the **Explorer.exe** process using the Task Manager. For more information, see [KB](#) article.

Index

A

- about this guide [5](#)
- active hosts, viewing [30](#)
- agent status [30](#)

C

- certificates
 - ePolicy Orchestrator deployment [17](#)
 - SCEP [20](#)
- conventions and icons used in this guide [5](#)

D

- discovery
 - ePolicy Orchestrator deployment [22](#)
 - methods [12](#)
- documentation
 - audience for this guide [5](#)
 - product-specific, finding [6](#)
 - typographical conventions and icons [5](#)

E

- ePolicy Orchestrator deployment
 - agent and extension packages [14](#)
 - assigning policy [25](#)
 - configuring certificates [17](#)
 - creating policy [21](#)

F

- firewall audit [30](#)

I

- integration [7](#)

L

- log files [30](#)

M

- McAfee ServicePortal, accessing [6](#)
- metadata [7](#)

R

- reports
 - Gateway Status [30](#)
 - Integrated Hosts [29](#)

S

- ServicePortal, finding product documentation [6](#)
- system requirements
 - ePolicy Orchestrator deployment [13](#)

T

- Technical Support, finding product information [6](#)

